AU/ACSC/112/2002-04

ACSC

AIR UNIVERSITY

PLANNING AND CONDUCTING OFFENSIVE COUNTERINFORMATION OPERATIONS

by

Virginia G. Swentkofske, Major, usaf

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Lieutenant Colonel Philip Bradley

Maxwell Air Force Base, Alabama

April 2002

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
00 APR 2002	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Planning And Conducting Offensive Counterinformation Operations	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air University Maxwell Air Force Base, Alabama**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**UU**	**53**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Page

Preface

I've experienced, or observed, first hand, many related challenges discussed in this paper while assigned as an intern to various duties within the National Security Agency and while assigned to several staff and operational assignments within the combat air forces and the Air Intelligence Agency. Many of the frustrations, delays and challenges I've experienced or observed seemed to evolve around a lack of established and accepted procedures (e.g. doctrine, TTPs, SPINS, ROE, etc.) which led to many questions and close scrutiny. Hopefully, this paper will help provide some direction and aid further discussion to anyone interested in this topic or working related issues.

I owe my sincerest thanks and appreciation to Lt Col Phil Bradley, my research advisor, for his help and advice. My family had to weather many marathon research and drafting sessions and the resulting dedicated and focused reading and writing that excluded good family attention and interaction. Thank you for your patience, support and love and, most of all, for occasionally fending for yourselves. Many thanks to everyone mentioned for making this paper possible.

Abstract

This paper examines the problems a joint force commander (JFC) faces when employing USAF OCI capabilities in his campaign plan. The intention is to address concerns as to how synchronized, interdependent events impact OCI operations conducted in a rapidly changing and highly compartmentalized environment. The focus is upon the command and control (C2) relationships and operational considerations such as formally established and documented procedures, target development, integration, synchronization and execution with the required intelligence and communications support. Execution is expected to occur under Title 10 authorities and from any point of access to the target with the intended effects occurring within the JFC's area of operations as an integrated and synchronized part of his campaign plan.

Methodology: A literature review of published literature, doctrine, the 1999 Unified Command Plan (UCP), and Air Combat Command documents begins this paper. Then, a discussion and analysis of joint and USAF doctrine and of operational direction, concepts and methods presented in the reviewed literature are employed with the intent to recommend or highlight operational concepts, security considerations, access appreciation, C2 relationships and attack planning methodologies. Related areas requiring further study and discussion are also noted.

Findings and Recommendations: Common terminology or approaches to OCI are not reflected in doctrine. Specifically, USAF's use of Information Warfare (IW) does not

equal the joint use of the term. Joint doctrine also recommends capabilities made available for specific uses be given directly to the JFC, while the USAF recommends all of its OCI capabilities be provided to the JFC through his COMAFFOR. The UCP and ACC's AOC CONOPS do not clarify matters. Thus, a JFC's ability to quickly determine how best to establish his C2 relationships with the apportioned or assigned OCI capabilities and requisite support and expertise is severely hampered. His planning staff's ability to realize the importance of certain liaison relationships between other DoD, national IC organizations, etc., establish them, provide guidance and JFC intent to them and monitor their cooperation for the sake of integration and synchronization within the campaign plan is also hampered.

A common understanding of the desired effects of the USAF OCI capabilities, target access, sufficient intelligence to enable the OCI capabilities and confidence in the capabilities' ability to deliver the desired effects for the time and circumstances specified are required. Other significant planning and operational factors include sufficient communications, adequate security scheme, access to the target and in-theater execution authority. Several specific recommendations on operational concepts, security, access, C2 relationships and attack planning methodologies are offered. Also, several related and important areas requiring further exploration are also identified.

Conclusions: USAF OCI capabilities will provide the JFC with excellent means to effect the enemy's information, information systems and decision-making processes, and will be more easily applied and more effective once understanding and familiarity with what OCI can and cannot do and how it provides that capability are understood. Hopefully, this paper helps provide some of the necessary understanding.

Chapter 1

Introduction

To subdue the enemy without fighting is the acme of skill. Thus, what is of supreme importance in war is to attack the enemy's strategy.

—Sun Tzu

Problem Statement

This paper will explore the intricacies a joint force commander (JFC) faces when choosing to employ USAF offensive counterinformation (OCI) capabilities within his campaign plan. The intention is to address concerns as to how synchronized, interdependent events impact USAF OCI operations within a campaign conducted in a rapidly changing and highly compartmentalized planning and execution environment. Specifically, this paper will explore and recommend command and control (C2) relationships and operational considerations such as go / no go criteria, target development, integration and synchronization, and the relevant intelligence and communication requirements to support these efforts.

Significance

OCI is basically a highly technical form of coercion. Technological advances in the realm of information resources management and the increasing world-wide reliance upon automated decision-making and information sharing make the possibility of favorably

shaping an enemy's observe, orient, decide and act (OODA) processes without having to mobilize and deploy forces into a theater of operations a true reality. Also, the ability to near-simultaneously coerce many decision-makers located across the globe through OCI methods with only intelligence planning factors impacting the response time would provide a great strategic advantage to the US, while also providing significant operational advantages to the supported joint forces.

Limitations and Scope

Since coercion through OCI could occur well before war or even during times of relative peace, the C2 structure for OCI operations may change as it occurs across this spectrum of operations. The challenges associated with determining and operating under proper legal authorities in peace or in crisis, while real and requiring exploration, are outside the scope of this paper. This paper focuses upon a JFC's employment of USAF OCI capabilities. Therefore, it will be assumed that OCI operations will occur under Title 10 authorities. Specifically, this paper will focus upon the JFC's C2 challenges and the planning and execution considerations associated with planning and conducting OCI from an access point to the target, located anywhere in the world, by geographically separated intelligence and operations elements, not necessarily located in the area(s) of operation, and thus, not co-located with the JFC's planners.

Once a JFC chooses to employ OCI capabilities within his area of operations and obtains the forces necessary to do so, a careful and detailed analysis of the operational environment is required to determine whose information and information systems to attack, why and how. Today, the many varied operational planning and intelligence expertise areas required to accomplish this task are scattered across the national

Intelligence Community (IC) and the Department of Defense (DoD). At present, portions of OCI planning occur in a highly compartmentalized environment (joint doctrine calls this special information operations (SIO)) which precludes timely data sharing and collaboration amongst the proper experts, planners, and operators and impacts the JFC's ability to integrate and synchronize OCI within his overall campaign plan. For instance, the communications technologies and protection measures employed by targeted leadership elements may require an OCI unit, not necessarily located in the area of operations, to receive a time-critical targeting update during execution from intelligence elements located either in the area of operations or outside the area of operations. If the intelligence elements and the operational elements do not have an established method to collect, identify and provide this critical information within operational execution requirements, then the attack's success is jeopardized. Thus, the development of standardized tactics, techniques and procedures, such as mission go / no go criteria, and a worldwide communications infrastructure are necessary to ensure the proper target(s) are found, fixed, tracked, targeted, engaged, attacked and assessed and to allow for appropriate collaboration, data-sharing and force protection.

Also, go / no go criteria are necessary during course of action (COA) development and approval since most effects of OCI have not been effectively modeled and simulated, demonstrated or exercised. This shortfall contributes to leadership and policy uncertainty since the OCI's effects and possible unintended consequences cannot be adequately shown or quantified and thus, control of those OCI capabilities becomes a highly sensitive and highly visible issue for national command authorities, policy-makers and the national Intelligence Community.

Currently, final authority to conduct sensitive attacks resides at the President of the United States (POTUS) or Secretary of Defense (SecDef) level of command. Thus, courses of action (COAs) containing those OCI options, must undergo extensive legal and policy reviews and intelligence gain / loss assessments. Once approved, any deviations must be evaluated and approved at the original approval authority level, unless the deviation is explicitly outlined in the original COA. The potential benefits of providing a strategic, parallel attack upon an enemy at almost a moment's notice without having to deploy attack assets and infrastructure are impeded by the amount of oversight and control due to unfamiliarity and understanding of the operational methodologies and control measures, the intended effects and possible unintended consequences.

All of the legal, policy, technical intelligence, planning, and operational experts work at different, geographically separated, organizations within the DoD and the national IC and at different security classification levels. Thus, their automated systems are not interoperable which precludes timely collaboration and information sharing and sometimes impacts timely release of certain critical data for planning and execution.

The events of September 11, 2001 revealed the need for better coordination and centralized direction of the many, varied and scattered federal and state government homeland defense capabilities. Similarly, OCI capabilities, expertise and enabling mechanisms, which exist within the DoD and the national IC, also have no centralized organization nor adequately detailed joint or service employment approaches to fully realize the potential capabilities' impact in a deliberate, much less a crisis action, planning and execution environment.

Chapter 2

Literature Review

Information Warfare is not the exclusive domain of the Air Force, or any service. Information technology advances will make dramatic changes in how this nation fights wars in the future.

—Sheila E. Widnall, Secretary of the US Air Force

Foundations

Before proceeding with an examination of planning and conducting OCI operations, some common terminology and understandings must be established. Exactly, what is information and why should it be attacked? To understand the answer to such questions, some definitions and ideas must be offered.

What is information? According to Secretary Widnall and General Fogleman, information is simply data and instructions. It is a result of perception or interpretation of observable facts or events, which gives the facts or events meaning.[1] Their definition is reflected in the current version of Joint Publication 1-02 and thus, will be the definition for this paper.[2]

[1] Cornerstones of Information Warfare, Widnall, Sheila E., Secretary of the US Air Force and General Ronald R. Fogleman. 6 November 2001, p. 2 found at http://www.af.mil/lib/corner.html
[2] Joint Publication 1-02, p. 202, 12 April 2001

Why attack information? Joint Pub 3-13 specifically states that the human decision making processes are the ultimate targets for offensive information operations.[3] Secretary Widnall and General Fogleman state that "competition for information is as old as human conflict."[4] According to General Fogleman and Secretary Widnall, quality information counters the fog of war, and in the military, it functions to support and enhance the employment of military forces. Thus, to deny, exploit, corrupt or destroy an enemy's information and its functions provides benefit to the attacker.[5]

How should information be attacked? Secretary Widnall and General Fogleman advocate direct and indirect attacks upon an enemy's information system to deny, exploit, corrupt or destroy their information and its functions.[6] Specifically, they advocate concentrating on the "military information function: any information function supporting and enhancing the employment of military forces."[7] In the case of OCI, an indirect or direct approach may be taken to conduct strategic attack and interdiction to either gain or affect an enemy's needed information for effective force employment.[8] Direct attack consists of direct access to and manipulation of an enemy's force employment information, usually through exploitation of vulnerabilities in data storage, access speeds (e.g. processing), and transport mechanisms.[9] Attack for the purpose of interdiction may alter an enemy planner's information and cause him to misdirect or misuse precious resources.[10] They continue by noting that attack capabilities "directly corrupt

[3] JP 3-13, *Joint Doctrine for Information Operations*, p. II-1, 9 Oct 1998.
[4] Cornerstones of Information Warfare, Widnall, Sheila E., Secretary of the US Air Force and General Ronald R. Fogleman. 6 November 2001, p. 2. found at http://www.af.mil/lib/corner.html
[5] ibid., p. 3.
[6] ibid.
[7] ibid.
[8] ibid., p. 4.
[9] ibid.
[10] ibid., p 7.

information without visibly changing the physical entity within which it resides."[11] It may only alter data or instructions. The immediate effects of which may not include visible changes. Thus, it directly impacts an enemy's information and information systems, not necessarily his perception or interpretation of it.

Retired Colonel John Warden's analysis, "The Enemy as a System", provides the best approach to analyzing an OCI problem. He recognizes the coercive nature of OCI capabilities and their strategic effects when he relates, "fighting is not the essence of war, nor even a desirable part of it. The real essence is doing what is necessary to make the enemy accept our objectives as his objectives."[12]

Problems

According to the USAF Information Warfare Mission Area Plan, command and control relationships, intelligence requirements and OCI planning methodologies exist, but need improvement.[13] Examination of joint and USAF doctrine reveals that disconnects exist with regard to offensive information operations and information warfare. US Space Command (USSPACE), which has Unified Command Plan (UCP) designated responsibility for computer network attack (a possible form of OCI) and Headquarters Air Combat Command (HQ ACC) have differing approaches towards providing OCI capabilities. These differences could result in USAF OCI capabilities, possibly within USSPACE's computer network attack organizations, Air Force Space Command (AFSPACE), or Air Combat Command (ACC), being provided to a JFC through different avenues. This could cause command and control and planning

[11] ibid.
[12] Warden, John A., III, Colonel, USAF. "The Enemy as a System." *National Planning Systems and Joint Campaign Planning, Vol 6*. p. 111. Air Command and Staff College: Maxwell AFB, AL January 2002.

concerns, especially from the JFC's point of view of synchronizing and integrating USAF OCI capabilities in a campaign plan.

USSPACE appears to view OCI applications from a global and a unified command to unified command viewpoint as evidenced by General Myers' comments on 5 January 2000, which follows the joint doctrine regarding supported and supporting unified command relationships.[14] Given current joint doctrine, any OCI capabilities residing under USSPACE would be provided to a JFC through that JFC's unified commander in chief (CINC). Thus, making it possible for any USAF capabilities residing within USSPACE's computer network attack organizations or AFSPACE to be apportioned or assigned directly to the JFC who then has the option to further delegate command and control of those capabilities within his command (e.g. JFACC / COMAFFOR).

HQ ACC follows USAF doctrine, which states that USAF warfighting capabilities are provided to a JFC through his commander, air force forces (COMAFFOR).[15] HQ ACC goes one step further and suggests that the JFC also consider making his COMAFFOR his JFACC, which allows the JFACC to capitalize upon the expertise and infrastructure resident within the COMAFFOR's AOC as reflected in its Air Operations Center (AOC) Concept of Operations (CONOPS).

Having USAF OCI capabilities possibly assigned, attached or made available directly to the JFC and directly to the JFC's COMAFFOR significantly impacts the unity of command and unity of effort for conducting OCI operations. The negative impact occurs since the C2, to include the planning methodologies, execution criteria and related intelligence and communications support is not clearly understood or agreed upon. This

[13] USAF IW MAP, p. A3, March 2001.
[14] General Myers, 5 Jan 2000 DoD Press Briefing Transcript.

situation could also adversely affect integration and synchronization of operations which are key to ensuring mission success.

Furthermore, USAF doctrine for information operations and warfare does not align well with current joint doctrine. Specifically, joint doctrine refers to offensive information operations (e.g. psychological operations (PSYOP), electronic warfare (EW), military deception, physical attack/destruction, maybe computer network attack (CNA), public affairs operations (PA), operations security (OPSEC), SIO and civil affairs (CA)) which implies execution of capabilities across the spectrum of operations, and possibly, not always under Title 10 authority.[16] In joint doctrine, IW is offensive IO conducted in crisis or conflict (including war), which implies under Title 10 authority. The USAF doctrine, on the other hand, discusses information warfare as counterinformation, further delineated as OCI (e.g. only PSYOP, EW, military deception, physical attack, CNA and PA; not OPSEC, SIO or CA) and defensive counterinformation (DCI).[17] Neither joint nor USAF doctrine address how any non-DoD OCI capabilities might be integrated or synchronized into a campaign plan or other efforts, but both recognize the necessity. Nor do they address how the USAF might integrate with other DoD capabilities to maximize any synergistic opportunities that may arise.

Also, no joint or USAF operational concept exists to describe when OCI planning and operations begin, how planning and operations are conducted, or the requirements for command and control, communications, computer, intelligence, surveillance and reconnaissance (C4ISR), personnel, security, legal / policy, logistics and maintenance support. Specifically, command and control relationships and operational considerations

[15] AFDD 2-5, *Air Force Doctrine Document 2-5*, p. 33. 17 February 2000.
[16] JP 3-13, *Joint Doctrine for Information Operations*, pp. I-10, I-11, II-5. 9 Oct 1998.

are not available for planners, operators and support elements. Examples of operational considerations include: inter-agency coordination, go / no go criteria, communication and tracking of current status amongst operational, planning and support elements working at differing security levels, and the relevant intelligence and communications requirements to support these efforts.

The USAF OCI capabilities and associated intelligence support are not located within one major command or numbered air force. The USAF intelligence elements reside within the Air Intelligence Agency, which resides within ACC. ACC also has Eighth Air Force and the 67th Information Operations Wing, which has OCI as part of its mission statement.[18] AFSPACE, however, has space control, which "may include denying" an enemy's use of his space assets and support to information-in-warfare as part of its mission statement.[19] Looking further, AFSPACE's 14th Air Force and its 21st Space Wing also contain these tasks as part of their mission statements.[20] Since, this paper's OCI definition could include space control; it is reasonable to infer that they could provide OCI capabilities.

Finally, OCI operations' execution does not necessarily require deployment of forces into the area of operations, nor do they necessarily preclude near-simultaneous support for multiple areas of operation (hence, multiple JFCs). Whether planned and executed from one area or multiple areas located around the globe, the C4ISR structure must support the data sharing and collaboration necessary for OCI mission success. This must

[17] AFDD-2-5, Air Force Doctrine Document 2-5, p. 12, 22 January 2002.
[18] 67IOW Mission Statement.
[19] AFSPACE Mission Statement.
[20] 14 AF Mission Statement.

occur regardless of which command(s) are supported, but also must address and support command relationships.

So the problems outlined for discussion fall into the broad categories of doctrine, operational concepts, targeting, integration and synchronization, and execution. Common throughout these categories are the challenges of attaining the proper detail of intelligence and providing it in the time and manner necessary for success—usually manifesting as security and access issues. Also common throughout, given the operation's worldwide nature, are the challenges of providing communications that allow timely collaboration and execution while abiding by the security constraints imposed due to the sensitive and highly controlled nature of the operations.

Chapter 3

Discussion and Analysis

How am I supposed to learn surgery if I can't dissect anything?

--Calvin
Bill Watterson's Calvin and Hobbes Comic Strip

Doctrine

Joint doctrine stresses the defense of our own information and information systems, first. It also categorizes information operations according to its sensitivity or to when conducted. If conducted via an especially sensitive means, it is classified as special information operations. Offensive information operations are conducted across the range of military operations while information warfare (IW) is conducted in crisis or conflict (including war). Joint information operations (IO) doctrine does not specify OCI as a subset capability. Instead, it discusses application of perception management actions, attack options and other contributing activities to produce a synergistic effect against elements of and enemy's information systems.[21]

The USAF, on the other hand, does not distinguish when OCI may occur, nor does it address sensitive activities. Its definitions also vary from the joint doctrine. In the USAF, IW is one of two subsets of IO and is "focused on the attack and defend

[21] JP 3-13, *Joint Doctrine for Information Operations*, pp. I-1, I-11, II-3, 9 Oct 1998.

functions". USAF doctrine states that joint terminology refers to "neutralizing or influencing adversary information activities", which is the air and space power function of counterinformation, which is also called IW. The USAF distinguishes and differentiates because, "in the joint arena IW is only conducted during contingencies while the USAF believes some parts of counterinformation are conducted every day." In USAF doctrine, counterinformation has offensive and defensive components. OCI includes actions taken to attack adversary information and information systems and is "essentially synonymous with the joint term for offensive information warfare." USAF doctrine also explicitly recognizes the vital importance of intelligence, surveillance and reconnaissance (ISR) activities, also referred to as information-in-warfare (IIW).[22]

The lack of common terminology or approaches to OCI reflected in joint and USAF doctrine significantly hampers a JFC's ability to determine how best to establish his command and control relationships with the available OCI capabilities and requisite support expertise. It also hampers his planning staff's ability to realize the importance of certain liaison relationships between other DoD, national IC organizations, etc., establish them, provide guidance to them on commander's intent and monitor their cooperation for the sake of integration and synchronization within the JFC's campaign plan.

Additionally, the 1999 UCP designates USSPACE with primary responsibility for computer network attack.[23] The intention was to provide a joint level, combatant command advocate for the development and fielding of computer network attack capabilities and resulting intelligence and communications support requirements and to

[22] AFDD 2-5, pp. 11-12. 22 January 2002.
[23] General Myers. 5 January 2000 DoD Press Briefing Transcript.

help resolve the national command level's legal and policy dilemmas that continue to arise during COA development and evaluation.

As highlighted in the “Problems” section of this paper, incongruent doctrinal approaches towards providing capabilities pose a potential problem to the JFC. The differences could complicate or confuse a JFC wishing to employ OCI capabilities because not all of the capabilities reside within service components, and of the capabilities that do reside within the USAF, they are not all located within AFSPACE. ACC has intelligence support and possibly other capabilities and provides its capabilities directly to a JFC’s COMAFFOR, per USAF doctrine.

If AFSPACE were to have OCI capabilities, that command might experience some headaches in designating the command relationships for them. As indicated earlier, any other USAF OCI capabilities would be presented to the JFC through his COMAFFOR. As part of USSPACE, AFSPACE may have to abide by the UCP 1999 tasking, which appears to direct that computer network attack and space control capabilities are provided by USSPACE directly to the supported combatant command CINC who then delegates that support to the JFC. Thus, presenting the JFC with the possibility of having USAF OCI capabilities presented directly to him through USSPACE and by ACC through his COMAFFOR. Without realizing it, the JFC could have USAF OCI planning elements and efforts at different levels of his command and due to its current compartmentalized nature, miss an opportunity to fully integrate and synchronize planning. Unity of command, unity of effort and unity of action could all be violated if some USAF OCI capabilities were assigned, attached or made available to the JFC while the rest were assigned, attached or made available to his COMAFFOR. This situation could present

OCI planners with significant hurdles to overcome to ensure synchronization and integration of OCI capabilities for maximum synergistic effect while avoiding intelligence loss or other complications during the course of operations.

Therefore, an examination of joint and USAF doctrine reveals incongruent doctrine for OCI capabilities, which leads to confusing and time-consuming efforts to establish streamlined and effective command and control relationships. Lost time and possibly ineffective or duplicative effort are then spent resolving this distraction. Planning, target development, integration and synchronization of USAF OCI capabilities within the JFC's campaign plan require dedicated effort without such distractions. This could occur due to lack of common approaches, vocabulary and understanding of what OCI is, what it can do, and how it is best employed. In other words, joint and USAF doctrine need to be congruent and easily understood by all the OCI planners, operators and support elements to ensure effectiveness, efficiency and success.

Operational Concepts

In order to execute OCI capabilities, certain conditions must exist. They include a common understanding of the desired effects of the USAF OCI capabilities, access to the intended target, sufficient intelligence about the intended target to enable the OCI capabilities and confidence in the capabilities' ability to deliver the desired effects for the time and circumstances specified. Other significant planning and operational factors include sufficient communications, adequate security scheme and in-theater execution authority. Communications should accommodate distributed, split and reachback collaborative planning support during COA and target development and assessment. The

classification and security control system employed to protect USAF OCI capabilities and operations should allow the proper planning, operational and support expertise to participate in the targeting and planning processes and quickly and freely exchange information and ideas. In-theater execution, while not an imperative, would greatly enhance the JFC's ability to respond to unfolding events and redirect OCI capabilities as necessary. This flexibility and responsiveness could prove very valuable in certain situations.

This paper's assumptions include executing USAF OCI capabilities from an access point located anywhere in the world with the effect(s) occurring in the JFC's area of operations. This allows for partnering with other services or agencies to obtain the necessary access and intelligence, but also introduces complications during planning and execution, which are discussed more extensively under "Execution".

The Air Force envisions planning and conducting aerospace operations in distributed, split and reachback environments.[24] For USAF OCI, the planning will have to occur in just such environments due to the vast number of service, joint, and intergovernmental agency OCI capabilities and expertise, not located in the area of operational responsibility / joint operations area (AOR / JOA), but necessary for planning and operational success. Therefore, supporting / supported roles need to be clearly defined during deliberate / crisis action planning, and commander's guidance and intent regarding the desired effects must be clearly articulated in order to bring the full potential of the OCIs to bear upon the targeted enemy.

The anticipated planning environments must allow for timely communications and data sharing for collaboration between geographically separated elements. Existing

USAF OCI capabilities are closely held. Also, they must be planned with extensive technical expertise not resident within the AOC, but accessible through the AOC. Therefore, the communications architecture must allow for the "push" of time-critical and highly sensitive information directly from organizations operating at a certain security level to the appropriate planning and operational elements, which are most likely operating at a different security level. Conversely, the planning and operational elements must also be able to "push" their information back to the supporting organizations. This is critical during COA development and assessment and can adversely impact the planning flow if it becomes too cumbersome or slow. Once mission execution begins and the release of any especially sensitive information is authorized for the operational elements, communications support could become critical to mission success.

The USAF also envisions conducting effects based planning within the AOC.[25] Effects based operations, is a planning and targeting approach described by Dr Maris McCrabb which provides a good foundation for conducting OCI.[26] As described in the Headquarters (HQ) Air Combat Command (ACC) Aerospace Operations Center (AOC) Concept of Operations (CONOPS), effects based planning consist of aerospace planning processes, which focus upon the desired strategic and operational effects the JFC tasks the JFACC to produce. These desired effects are articulated in COAs considered by the JFC in his estimate process.[27] Desired OCI effects could include destruction, disruption or deception of an enemy's information and decision-making capabilities where disruption includes denial and degradation of capabilities.

---

[24] USAF AOC CONOPS, 9 March 2001, p. 4.
[25] Ibid., p. 6.
[26] EBO CONOPs, ver2.0, p. 7.
[27] USAF AOC CONOPS, 9 March 2001, p.6.

Targeting

According to Waltz in Information Warfare Principles and Operations, information may be attacked at the perceptual, information or physical levels.[28] Since perceptual level attacks usually include perception management through psychological operations and deception, the OCI portion, which targets the observed information and its transport and processing, will require close integration and synchronization with the psychological operations and deception plans to ensure a united, synergistic attack occurs. When the information infrastructure is attacked, intelligence on where the information of interest is collected, how it is transported, processed, analyzed, displayed, stored and collated for the decision-makers is of vital importance. The steps taken to collect the necessary level of intelligence to answer these questions will also enable certain OCIs and in some cases, may even preclude a revisit for the actual attack. In those cases, the OCI operators and the intelligence collection operators will need to work very closely with each other to ensure intelligence collection and attack operations complement each other and don't cancel each other.

The HQ ACC AOC CONOPS states that, "dynamic decision-making is the most challenging process in the AOC."[29] And further states that:

> During the normal course of execution, events follow the "plan" generated through the processes described in the AOC CONOPS, and in accordance with the Targeting Cycle described in JP 3-56.1. This cycle (Guidance, Target Development, Weaponeering, Force Application, Execution Planning/Execution, and Combat Assessment) occurs throughout the battle rhythm largely determined by the JFC. When a dynamic event occurs, this cycle becomes time-compressed. The operational kill chain (find, fix, track, target, engage, assess) occurs during the course of dynamic execution. Every step of the Targeting Cycle occurs in a greatly

[28] Waltz, *Information Warfare Principles and Operations*, p. 240.
[29] USAF AOC CONOPS, 9 March 2001, p. 13.

> compressed timeframe during dynamic events. Information technologies can improve the ability to see, confidently identify, prioritize, assign attack assets, strike and assess mission results. Further, information technology could provide the decision-making tools, decision support systems, and simulations to enable commanders to make better and quicker decisions. Decision aids should support planning and recommended COAs within the compressed timelines involved with dynamic events.[30]

The nature of the OCI operational environment will necessitate dynamic targeting for extensive and extended OCI operations. As the US increases its OCI capabilities and demonstrates it through use, targeted entities and interested observers will adapt available technology and develop their own security and protection measures to lessen their vulnerability to attack. Technology will allow these measures to become active or change their parameters just prior to or during the course of the OCI. Thus, USAF OCI capabilities must assure their continued success by having the ability to detect and adapt to any changes from the planned (or expected) target environment. Again, this will require extensive intelligence and communications expertise and support during the attack, as well as previously coordinated execution authority. The USAF describes this capability as predictive battlespace awareness (PBA).

Specifically, PBA, according to the US Marine Corps and the USAF observations from recent aerospace operations, demonstrates a structured intelligence, surveillance and reconnaissance (ISR) process that synchronizes national, theater, and tactical assets into one ISR strategy and optimizes ISR operations.[31] Thus, PBA is a considerable force multiplier. PBA results from combining Target System Analysis (TSA), Intelligence Preparation of the Battlefield (IPB), ISR planning and synchronization, and ISR employment into a coherent framework that maximizes the capabilities of ISR assets

[30] Ibid.

across the spectrum of operations and in all environments. It is through the integration of these traditionally separate components that provides commanders the capability to shift ISR assets from a collection to a targeting mind-set for those anticipated events that predictive analysis allows. This detailed level of understanding of the battlespace will minimize the time from target detection to attack, particularly against time-sensitive targets / time-critical targets (TST/TCTs). PBA ultimately allows the commander to select the optimum means to achieve desired effects, seize and maintain the initiative and, most importantly, continuously evaluate generated effects, conditions, and COA allowing for the selection of the optimum friendly COA. PBA is also the basis for future architectures to integrate advanced air and space-based platforms capable of machine-level interaction to help perform surveillance, reconnaissance, and command and control functions to precisely locate critical targets and significantly improve global engagement capabilities. [32]

To prepare for a successful OCI, extensive targeting development work must occur. First an understanding of the operational environment must be developed, normally referred to by the US Army and the US Marine Corps as IPB. Where OCI planning is concerned, IPB consists of understanding the information, information systems, and information and decision-making processes of the targeted leadership / decision-makers to include noting redundancies, protection and security measures, locations, required enabling technical information and access points (vulnerabilities). Once targeted entities and desired effects are identified, then in-depth, detailed targeting development can occur to include the identification of opportunities to integrate and synchronize OCIs with other

[31] Millennium Challenge CONOPS, p. 6.
[32] Ibid.

attacks to maximize synergism and achieve the overall desired effect at the targeted entity. It is important to note that OCIs will almost always need to occur in conjunction with other attacks to achieve the desired effect.

Integration and Synchronization

Integration and synchronization into the campaign plan are very difficult to achieve in OCI operations for a variety of reasons. For instance, doctrine does not provide a common understanding of capabilities. Also, capabilities are planned and executed in a highly compartmentalized manner. Therefore, OCI planners, operators and associated support experts in intelligence and communications are not necessarily aware of whom to coordinate with or how to coordinate with them in a properly secured manner. Also, USAF OCI capabilities may need to closely coordinate with non-USAF OCI assets. If they are operating under different security constraints, difficulties quickly arise and valuable time is lost.

The value of having one commander responsible for all OCI operations and a designated staff single point of entry for planning and executing an integrated and synchronized OCI plan into the overall theater campaign plan cannot be overstressed. The COMAFFOR plans to provide an information warfare flight within his AOC. His AOC already plans to conduct distributed, split, and reachback operations, therefore implying that it will have the C4ISR assets and support necessary to accomplish such missions. The JFACC, then, is a logical person to designate as the commander for all OCI capabilities to capitalize upon and allow maximum synergism, assuming the JFACC is the COMAFFOR. If the JFACC is not also the COMAFFOR, and then the COMAFFOR should be the designated commander for all of the USAF OCI capabilities

assigned or apportioned to the JFC. This will ensure intelligence gain / loss assessments and targeting activities do not preclude the access needed for successful OCI operations.

OCI operations will require integration and synchronization into the JFC's campaign plan to maximize its synergistic contributions to achieve the overall effect of destroying, disrupting or deceiving the targeted entities (e.g. leaders or decision-makers). For instance, OCI could help achieve a JFC's goals for attack upon enemy leadership, command and control, upon his integrated air defenses, or any other centralized and automated decision-making and communication process. OCI may also help achieve a JFC's goals for conducting PSYOP or deception. During a pop-up combat search and rescue operation (CSAR), OCI might disrupt the enemy forces' ability to coordinate their response efforts to find and capture downed crewmembers.

Thus, integration and synchronization are necessary. Specifically, they can: achieve access to the targeted entities; prevent detection of our capabilities; notify the OCI operators of changes to planned attack parameters (e.g. loss or change of access, security or protection measures, target location or technical parameters); or ensure ISR assets collect and report any effects.

Execution

Execution of OCI operations will need to occur in a decentralized manner. The execution element(s) may be located out of the area of operations or co-located with other enabling capabilities (e.g. access points, intelligence support). OCI has a time-sensitive targeting and time-critical targeting nature. It also has a high level of command and control over its operations. Therefore, go / no go criteria must be carefully considered and clearly stated as special instructions (SPINS) or rules of engagement (ROE). These

SPINS and ROE must be made available for all planning, operational and support elements to ensure the integrity of integration and synchronization, to ensure the intended synergism of effects occur, and to ensure that operators are allowed maximum responsiveness and flexibility. SPINS and ROE also minimize the risk of intelligence loss, compromise, detection or interception. Go / no go criteria should provide the OCI operator with explicit guidance on what he is to do when confronted with unexpected circumstances. Unexpected circumstances could include a loss or change of access, loss or changes of ability to report mission status during execution, change in expected target protection, security or technical parameters, or target location change. Careful and thorough consideration of these guidelines and their documentation, to include standardized formats, wording, and tactics, techniques and procedure, during planning development will aid in securing JFC command authority for execution and increase flexibility and responsiveness even more. During execution the compartmentalized nature of OCI and the likelihood that the dynamic operational environment will demand or cause changes to the OCI plan could complicate the coordination and oversight of the mission(s)' outcome with the other integrated and synchronized portions of the campaign.

Chapter 4

Suggested Next Steps

> *Thus, those skilled in war subdue the enemy's army without battle. They capture his cities without assaulting them and overthrow his state without protracted operations.*
>
> --Sun Tzu

Operational Concept Recommendations

The following operational concept recommendations seek to enable the JFC to command and control the OCI capabilities assigned and apportioned to him and to maximize opportunities for integration and synchronization of synergistic effects.

First, legal authorities and policies to execute OCI operations in theater without first seeking POTUS or SecDEF approval would provide the JFC with better flexibility and responsiveness to dynamic situations as they occur. Second, doctrine congruency between the joint and USAF doctrine and a clarification of the command relationships of AFSPACE capabilities to the JFC and JFACC are necessary. Third, outline clear, simple command and control relationships for all OCI capabilities (e.g. includes USAF, other DoD and national IC) brought to bear within a theater. Fourth, set well established standardized and practiced procedures for distributed, split and reachback operations. Fifth, establish common targeting methodologies and standardized intelligence requirements to establish initial characteristics of enemy information architectures,

procedures, policies, etc, to identify common vulnerabilities and access methods and to identify any noteworthy changes.

Security Recommendations

Also, establish a common classification access to allow the OCI operators, planners, intelligence and acquisition communities, and technical experts (e.g. communications and computers, space, SOF, PSYOPS, deception, etc.) to perform the following collaborative functions in a distributed, virtual, computerized environment. Collaborate to analyze and refine the target environment and identify vulnerabilities. Also, collaborate for COA proposal and evaluation and intelligence gain / loss assessments. Visualize synchronization and integration with the overall theater campaign plan to understand impacts to the original plan when new or changed courses of action are incorporated. Visualization is also an important aid for understanding the impact of environmental changes (e.g. lost or changed access methods, new / unknown security measures) during mission execution. Finally, evaluate the possible unintended consequences for proposed attacks.

Access Recommendations

Access to the target(s) will dictate from where capabilities are employed. From a basing and deployment standpoint, suggest locating most OCI operational capabilities within the US with the ability to deploy elements to any worldwide access point(s) necessary for mission accomplishment. These deployment teams should include the necessary C4ISR support and expertise tailored for the assigned mission(s) (e.g. PSYOPS, deception, space, SOF, intelligence, computer and communications). Of

course this scheme will only work reliably if the deployment teams have and abide by strict command and control measures since no commander would want a deployed team to execute its mission "in the blind". At a minimum, once the team is in place, C4ISR should be established to ensure no changes to the mission parameters, SPINS or ROE and to alert any other attack elements depending upon this team or supporting this team. ISR required for mission success (e.g. pre-strike reconnaissance, mission monitoring, post-strike reconnaissance and combat / battle damage assessment) also requires notification of in-place and ready to execute deployment teams since their collection and reporting priorities may change if there is no OCI mission to support.

C2 Recommendations

The scope of this paper limited its discussion to OCI operations conducted under Title 10 authorities. Therefore, using the joint and USAF doctrine and the HQ ACC AOC CONOPS guidance, recommend the JFC be designated the supported commander with the national IC supporting him. If the JFC is not CINCUSSPACE, then recommend USSPACE also support the JFC, but assign, attach or make available any OCI capabilities that may exist in its computer network attack organizations or AFSPACE to the JFC's COMAFFOR. For any other USAF OCI capabilities, recommend they also be assigned, attached or made available to the JFC's COMAFFOR. Specifically, the command and control relationships to the COMAFFOR should include tactical control (TACON) for out of theater USAF capabilities and operational control (OPCON) for in theater USAF capabilities. For any non-USAF OCI capabilities executed in an AOR / JOA, recommend that they be OPCON to COMAFFOR to benefit from the C4ISR support and information operations expertise resident within his AOC. When OCI assets

are supporting PSYOP, deception plans or CSAR missions, recommend the COMAFFOR, who has OPCON of in-theater assets and TACON of out of theater assets, consider assigning TACON as necessary (e.g. JPOTF).

Attack Planning Methodology Recommendations

At the information infrastructure level, the amount and level of detail required to understand the enemy's OODA processes and then to get inside it and stay inside it is phenomenal. To complicate matters, that environment is highly dynamic. Therefore when planning OCI operations it is very important to understand the enemy's system redundancy and his vulnerabilities to disruption by other means. As such, the following is a suggested OCI planning methodology.

1. Identify the desired outcome (e.g. prevent leader XX from receiving and / or communicating certain information for time period yyyy:mm:dd:hh:mm:ss.s to yyyy:mm:dd:hh:mm:ss.s with ##% probability of detection or probability of intercept).

2. Determine which information and / or information system(s) are to be attacked (e.g. current friendly / enemy force status). For example, answer / consider the following: how does leader XX receive the targeted information; what exactly is in the targeted information; from where / whom is it received; to whom / where is it communicated (e.g. situation displays from encrypted broadcasts or radio, text, phone or fax messages from subordinate units, etc).

3. Determine primary, secondary and tertiary means leader XX uses to receive, process and transmit the information to be attacked (e.g. cell phone, pager, landline, RF, PSTN, fiber optic, dial-up access, LAN / WAN, etc.).

4. Determine the technical characteristics of these means for the transmission, processing and storage of information of interest (e.g. encryption, multiplexing, encoding, hardware make and model, software versions, etc).

5. Identify vulnerabilities in information structure(s) with the targeted information.

6. Identify access methods available to target the vulnerabilities.

7. Identify OCI capabilities that can leverage the access mechanisms, the vulnerabilities, and can achieve the desired effects

8. Develop courses of action.

9. Follow the standard courses of action approval and implementation processes.

Summary

Suggested next steps for further research and refinement of OCI included recommendations on operational concepts, security, access, command and control and planning methodologies. These recommendations are not intended as an all-inclusive list, but as indicators of the more pressing issues that require resolution or close monitoring by the JFC to ensure successful operations.

Chapter 5

Findings and Conclusions

The real target in war is the mind of the enemy commander, not the bodies of his troops.

-- Captain Sir Basil Liddell Hart

Areas Requiring More Exploration

As noted in the scope and limitations, OCI may occur throughout the spectrum of conflict. If it is specifically used to coerce national leaders, policy or decision-makers, that could occur outside of Title 10 authorities. The command and control relationships and legal authorities associated with such operations require further examination, especially if USAF OCI capabilities or expertise are tasked.

As mentioned in the "Execution" section and recommended in the "Operational Concept" section, JFC level execution authority of OCI operations would greatly increase responsiveness and flexibility. Thus, how to obtain the legal authorities and policies for in-theater execution approval requires further discussion beyond the need for documented standardized procedures discussion offered in this paper.

This paper focused purely upon a JFC's planning and conducting of OCI operations within his area of operations. Conducting OCI operations while defending against similar attacks is out of scope. However, since the US military and national level command elements are heavily dependent upon integrated information architecture,

defending our information processes and systems from attack is of vital importance. Thus, consideration and discussion of how to execute OCI in a highly dynamic environment where the JFC / JFACC is defending his systems from enemy attacks both from within his networks and from the outside is necessary.

Research for this paper discovered that the USSPACE's UCP 1999 responsibilities for computer network attack could present a situation where its OCI capabilities (e.g. computer network attack, space control, etc.) could be apportioned directly to the supported JFC through USSPACE. This is contrary to USAF's doctrinal recommendation to present its capabilities to the supported JFC through his COMAFFOR. Thus, AFSPACE may find itself in a quandary as to which way to present it's capabilities. This paper supports the USAF doctrinal approach since it focused upon USAF OCI capabilities. However, consideration must be given to synergistic cooperation between several DoD services and agencies, the national IC, and other organizations providing support or capabilities with the command and control challenges that situation presents, especially if not operating under Title 10 authorities. Thus, recommend further investigation of ways to resolve the joint and USAF doctrinal differences and ways to resolve the apparently differing intra-service approaches towards providing USAF capabilities to the JFC.

Conclusion

This paper explored the intricacies a JFC faces when choosing to employ USAF OCI capabilities within his campaign plan. Specifically, it analyzed OCI planning, integration, synchronization and execution within today’s compartmentalized environment. At the operational level, doctrinal and classification problems complicate

the C2, planning and targeting processes and intelligence and communications support requirements. This impacts the effectiveness of planners' and operators' ability to synchronize and integrate OCI capabilities within the overall campaign plan and limits their flexibility and responsiveness.

A breakdown in doctrinal congruency exists between the joint doctrine and USAF doctrine. This directly impacts command and control relationships and supported and supporting relationships. These in turn, affect the development and implementation of standardized guidance to include SPINS and ROEs, common targeting methodologies, standing intelligence requirements, and access mechanisms. Classification schemes also impact the planners, operators and intelligence communities ability to share vital information within a common planning environment. In particular, access mechanisms and vulnerability analysis identification information may not be available to the USAF OCI planners and operators in a timely manner.

Following the literature review and discussion and analysis of doctrine, operational concepts, targeting, integration, synchronization and execution, recommendations were presented to address the problems identified and discussed. These recommendations included operational concepts, command and control relationships and attack planning methodologies. Related areas requiring further study and discussion where then noted. USAF OCI capabilities will provide the JFC with excellent means to effect the enemy's information and decision-making processes, and will be more easily applied and more effective once understanding and familiarity with what OCI can and cannot do and how it provides that capability are understood. Hopefully, this paper helps provide some of the necessary understanding.

Glossary

8AF	Eighth Air Force
14AF	Fourteenth Air Force
21SW	Twenty-first Space Wing
67IOW	Sixty-seventh Information Operations Wing
ACC	Air Combat Command
ACSC	Air Command and Staff College
AF	Air Force
AFSPACE	Air Force Space Command
AIA	Air Intelligence Agency
AOC	Air Operations Center
AOR	Area of Responsibility
AOO	Area of Operations
AU	Air University
C2	Command and Control
C4ISR	Command, Control, Communications and Computers, Intelligence, Surveillance and Reconnaissance
CA	Civil Affairs Operations
CI	Counterinformation
CINC	Commander in Chief
CNA	Computer Network Attack
COA	Course of Action
COCOM	Combatant Command
COG	Center of Gravity
COMAFFOR	Commander, Air Force Forces
CONOPS	Concept of Operations
CSAR	Combat Search and Rescue
DCI	Director of Central Intelligence
DIRNSA	Director, National Security Agency
DOD	Department of Defense
EBO	Effects Based Operations
HQ	Headquarters
I&W	Indications and Warning

IA	Information Assurance
IC	Intelligence Community
IIW	Information in Warfare
IPB	Intelligence Preparation of the Battlefield
IO	Information Operations
IOW	Information Operations Wing
ISR	Intelligence, Surveillance and Reconnaissance
IW	Information Warfare
J-2	Intelligence Directorate of a Joint Staff
J-3	Operations Directorate of a Joint Staff
J-5	Plans Directorate of a Joint Staff
J-6	Command, Control, Communications and Computer Systems Directorate of a Joint Staff
JFACC	Joint Force Air Component Commander
JFC	Joint Force Commander
JOA	Joint Operations Area
JPOTF	Joint Psychological Operations Task Force
JTF	Joint Task Force
JTTP	Joint Tactics, Techniques and Procedures
OCI	Offensive Counter Information
OODA	Observe, Orient, Decide and Act
OPCON	Operational Control
OPSEC	Operations Security
PA	Public Affairs Operations
PBA	Predictive Battlespace Awareness
POTUS	President of the United States
PSTN	Public Switched Telephone Network
PSYOP	Psychological Operations
RF	Radio Frequency
ROE	Rules of Engagement
SecDef	Secretary of Defense
SIO	Special Information Operations
SOF	Special Operations Force
SPINS	Special Instructions
SW	Space Wing
TACON	Tactical Control
TCT	Time Critical Targeting
TSA	Target System Analysis
TST	Time Sensitive Targeting
TTP	Tactics, Techniques and Procedures

UCP	Unified Command Plan
USA	United States Army
USAF	United States Air Force
USJFC	United States Joint Force Command
USMC	United States Marine Corps
USSOCOM	United States Special Operations Command
USSPACECOM	United States Space Command

Definitions

access. Ability to directly or indirectly intrude into a targeted information system and capture or affect its information. (Waltz, Information Warfare Principles and Operations)

allocation. In a general sense, distribution of limited resources among competing requirements for employment. Specific allocations (e.g. air sorties, nuclear weapons, forces and transportation) are described as allocation of air sorties, nuclear weapons, etc. See also allocation (air); allocation (nuclear); allocation (transportation); apportionment. (JP 1-02)

allotment. The temporary change of assignment of tactical air forces between subordinate commands. The authority to allot is vested in the commander having combatant command (command authority). (JP 1-02)

apportionment. In the general sense, distribution for planning of limited resources among competing requirements. Specific apportionments (e.g. air sorties and forces for planning) are described as apportionment of air sorties and forces for planning, etc. See also allocation; apportionment (air). (JP 1-02)

area of operations. An operational area defined by the joint force commander for land and naval forces. Areas of operation do not typically encompass the entire operational area of the joint force commander, but should be large enough for component commanders to accomplish their missions and protect their forces. Also called AO. See also area of responsibility; joint operations area. (JP 1-02)

assign. 1. To place units or personnel in an organization where such placement is relatively permanent, and/or where such organization controls and administers the units of personnel for the primary function, or greater portion of functions, of the unit or personnel. 2. To detail individuals to specific duties or functions where such duties or functions are primary and/or relatively permanent. (JP 1-02)

attach. 1. The placement of units or personnel in an organization where such placement id relatively temporary. 2. The detailing of individuals to specific functions where such functions are secondary or relatively temporary, e.g., attached for quarters and rations; attached for flying duty. (JP 1-02)

battle damage assessment. The timely and accurate estimate of damage resulting from the application of military force, either lethal or non-lethal, against a predetermined objective. Battle damage assessment can be applied to the employment of all types of weapon systems (air, ground, naval and special forces weapon systems) throughout the range of military operations. Battle damage assessment is primarily an intelligence responsibility with required inputs and coordination from the operators. Battle damage assessment is composed of physical damage assessment, functional damage assessment and target system assessment. Also called BDA. See also combat assessment. (JP 1-02)

battlespace. The commander's conceptual view of the area and factors which he must understand to successfully apply combat power, protect the force and complete the mission. It encompasses all applicable aspects of air, sea, space and land operations that the commander must consider in planning and executing military operations. The battlespace dimensions can change over time as the mission expands or contracts, according to operational objectives and force composition. Battlespace provides the commander a mental forum for analyzing and selecting courses of action for employing military forces in relationship to time, tempo and depth. (AFDD 1)

campaign plan. A plan for a series of related military operations aimed at accomplishing a strategic or operational objective within a given time and space. (JP 1-02)

centers of gravity. Those characteristics, capabilities, or localities from which a military force derives its freedom of action, physical strength or will to fight. (JP 1-02) (They exist at the strategic, operational and tactical levels of war. --offered for clarity within the USAF). (AFDD-2)

chain of command. The succession of commanding officers from a superior to a subordinate through which command is exercised. Also called command channel. (JP 1-02)

clandestine operation. An operation sponsored or conducted by governmental departments or agencies in such a way as to assure secrecy or concealment. A clandestine operation differs from a covert operation in that emphasis is placed on concealment of the operation rather than on concealment of identity of sponsor. In special operations, an activity may be both covert and clandestine and may focus equally on operational considerations and intelligence-related activities. (JP 1-02)

combat assessment. The determination of the overall effectiveness of force employment during military operations. Combat assessment is composed of three major components, (a) battle damage assessment, (b) munitions effects assessment, and (c) reattack recommendations. The objective of combat assessment is to identify recommendations for the course of military operations. The J-3 is normally the single point of contact for combat assessment at the joint force level, assisted by the joint force J-2. Also called CA. (JP 1-02)

combat power. The total means of destructive and / or disruptive force which a military unit / formation can apply against the opponent at a given time. (JP 1-02)

combat search and rescue. A specific task performed by rescue forces to effect the recovery of distressed personnel during war or military operations other than war. Also called CSAR. (JP 1-02)

combatant command. A unified or specified command with a broad continuing mission under a single commander established and so designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff. Combatant commands typically have geographic or functional responsibilities. (JP 1-02)

combatant commander. A commander in chief of one of the unified or specified combatant commands established by the President. See also combatant command. (JP 1-02)

command and control. The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission.

Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities and procedures employed by a commander in planning, directing, coordinating and controlling forces and operations in the accomplishment of the mission. Also called C2 (JP 1-02).

command, control, communications, and computer systems. Integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities and communications designed to support a commander's exercise of command and control across the range of military operations. Also called C4 systems. (JP 1-02)

command relationships. The interrelated responsibilities between commanders, as well as the operational authority exercised by commanders in the chain of command; defined further as combatant command (command authority), operational control, tactical control or support (JP 1-02)

common operating environment. Automation services that support the development of the common reusable software modules which enable interoperability across multiple combat support applications. This includes segmentation of common software modules from existing applications, integration of commercial products, development of a common architecture and development of common tools for application developers. (JP 1-02)

communications. A method or means of conveying information of any kind from one person or place to another. (JP 1-02)

computer. An electronic machine that performs high-speed mathematical or logical calculations or that assembles, stores, correlates, or otherwise processes and prints information derived from coded data in accordance with a predetermined program.

computer network attack. Operations to disrupt, deny, degrade or destroy information resident in computers and computer networks or the computers and networks themselves. Also called CNA. (JP 1-02).

concept of operations. A verbal or graphic statement, in broad outline, of a commander's assumptions or intent in regard to an operation or series of operations. The concept of operations frequently is embodied in campaign plans and operation plans; in the latter case, particularly when the plans cover a series of connected operation to be carried out simultaneously or in succession. The concept is designed to give an overall picture of the operation. It is included primarily for additional clarity of purpose. Also called commander's concept. (JP 1-02)

control. 1. Authority which may be less than full command exercised by a commander over part of the activities of subordinate or other organizations. (JP 1-02)

coordinating authority. A commander or individual assigned responsibility for coordinating specific functions or activities involving forces of two or more Military Departments, two or more joint force components or two or more forces of the same Service. The commander or individual has the authority to require consultation between the agencies involved, but does not have the authority to compel agreement. In the event that essential agreement cannot be obtained, the matter shall be referred to the appointing authority. Coordinating authority is a consultation relationship, not an authority through which command may be exercised. Coordinating authority is more applicable to planning and similar activities than to operations.

counterinformation. Counterinformation seeks to establish a desired degree of control in information functions that permits friendly forces to operate at a given time or place without prohibitive interference by the opposing force. (AFDD 2-5)

counterspace. Those offensive and defensive operations conducted by air, land, sea, space, special operations and information forces with the objective of gaining and maintaining control of activities conducted in or through the space environment. (AFDD 1)

coup de main. An offensive operation that capitalizes on surprise and simultaneous execution of supporting operations to achieve success in one swift stroke. (JP 1-02)

course of action. 1. A plan that would accomplish, or is related to, the accomplishment of a mission. 2. The scheme adopted to accomplish a task or mission. It is a product of the Joint Operation Planning and Execution System concept development phase. The supported commander will include a recommended course of action in the commander's estimate. The recommended course of action will include the concept of operations, evaluation of supportab8ility estimates of supporting organizations, and an integrated time-phased data base of combat, combat support and combat service support forces and sustainment. Refinement of this data base will be contingent on the time available for course of action development. When approved, the course of action becomes the basis for the development of an operations plan or operation order. Also called COA. (JP 1-02)

crisis action planning. 1. The Joint Operation Planning and Execution System process involving the time-sensitive development of joint operation plans and orders in response to an imminent crisis. Crisis action planning follows prescribed crisis action procedures to formulate and implement an effective response within the time frame permitted by the crisis. 2. The time-sensitive planning for the deployment, employment, and sustainment of assigned and allocated forces and resources that occurs in response to a situation that may result in actual military operations. Crisis action planners base their plan on the circumstances that exist at the time planning occurs. Also called CAP. (JP 1-02)

deception. Those measures designed to mislead the enemy by manipulation, distortion or falsification of evidence to induce him to react in a manner prejudicial to his interests. (JP 1-02).

decisive point. A geographic place, specific key event, critical system or function that allows commanders to gain a marked advantage over an enemy and greatly influence the outcome of an attack. (JP 1-02)

deliberate planning. 1. The Joint Operation Planning and Execution System process involving the development of joint operation plans for contingencies identified in joint strategic planning documents. Conducted principally in peacetime, deliberate planning is accomplished in prescribed cycles that complement other Department of Defense planning cycles in accordance with the formally established Joint Strategic Planning System. 2. A planning process for the deployment and employment of apportioned forces and resources that occurs in response to a hypothetical situation. Deliberate planners rely heavily on assumptions regarding the circumstances that will exist when the plan is executed. (JP 1-02)

direct effect. Result of actions with no intervening effect or mechanism between act and outcome. Direct effects are usually immediate and easily recognizable. (AFDD 2-1)

doctrine. Fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgement in application. (JP 1-02)

indirect effect. Result created through an intermediate effect or mechanism to produce the final outcome, which may be physical or psychological in nature. Indirect effects tend to be delayed and may be difficult to recognize. (AFDD 2-1)

information. 1. Facts, data or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation. (JP 1-02)

information-in-warfare. Involves the Air Force's extensive capabilities to provide global awareness throughout the range of military operations based on integrated intelligence, surveillance and reconnaissance assets; information collection/dissemination activities; and global navigation and positioning, weather and communications capabilities. (AFDD 2-5)

information operations. Actions taken to affect adversary information and information systems while defending one's own information and information systems. (DODD S-3600.1) The USAF believes that in practice a more useful working definition is: (Those actions taken to gain, exploit, defend or attack information and information systems and includes both information-in-warfare (IIW) and information warfare (IW)--applies only to USAF and is offered for clarity. (AFDD-2)

information warfare. Information operations conducted during time of crises or conflict to achieve or promote specific objectives over a specific adversary or adversaries. (DODD S-3600.1) The USAF believes that, because the defensive component of IW is always engaged, a better definition is: Information operations conducted to defend one's own information and information systems, or to attack and affect an adversary's information or information systems--applies only to USAF and is offered for clarity. (AFDD-2)

integration. 1. In force projection, the synchronized transfer of units into an operational commander's force prior to mission execution. 2. The arrangement of military forces and their actions to create a force that operates by engaging as a whole. 3. In photography, a process by which the average radar picture seen on several scans of the time base may be obtained on a print, or the process by which several photographic images are combined into a single image. (JP 1-02)

intelligence. 1. The product resulting from the collection, processing, integration, analysis, evaluation and interpretation of available information concerning foreign countries or areas. 2. Information and knowledge about an adversary obtained through observation, investigation, analysis or understanding. (JP 1-02)

intelligence preparation of the battlespace. An analytical methodology employed to reduce uncertainties concerning the enemy, environment and terrain for all types of operations. Intelligence preparation of the battlespace builds an extensive data base for each potential area in which a unit may be required to operate. The data base is then analyzed in detail to determine the impact of the enemy, environment and terrain on operations and presents it in graphic form. Intelligence preparation of the battlespace is a continuing process. Also called IPB. (JP 1-02)

interagency coordination. Within the context of Department of Defense involvement, the coordination that occurs between elements of the Department of Defense and

engaged US Government agencies, nongovernmental organizations, private voluntary organizations and regional and international organizations for the purpose of accomplishing an objective. (JP 1-02)

interoperability. 1. The ability of systems, units or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together. 2. The condition achieved among communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and / or their users. The degree of interoperability should be defined when referring to specific cases. (JP 1-02)

joint decision support tools. Joint decision support tools are a compilation of processes and systems developed from the application of maturing leading edge information systems technologies that provide the warfighter and the logistician with the means to rapidly plan, execute, monitor and replan logistic operations in a collaborative environment that is responsive to operational requirements. Also called JDST. (JP 1-02)

joint force air component commander. The joint force air component commander derives authority from the joint force commander who has the authority to exercise operational control, assign missions, direct coordination among subordinate commanders, redirect and organize forces to ensure unity of effort in the accomplishment of the overall mission. The joint force commander will normally designate a joint force air component commander. The joint force air component commander's responsibilities will be assigned by the joint force commander (normally these would include, but not be limited to, planning, coordination, allocation and tasking based on the joint force commander's apportionment decision). Using the joint force commander's guidance and authority, and in coordination with other Service component commanders and other assigned or supporting commanders, the joint force air component commander will recommend to the joint force commander apportionment of air sorties to various missions or geographic areas. Also called JFACC. See also joint force commander. (JP 1-02)

joint force commander. A general term applied to a combatant commander, subunified commander, or joint task force commander authorized to exercise combatant command (command authority) or operational control over a joint force. Also called JFC. See also joint force. (JP 1-02)

joint operations area. An area of land, sea, and airspace, defined by a geographic combatant commander of subordinate unified commander, in which a joint force commander (normally a joint task force commander) conducts military operations to accomplish a specific mission. Joint operations areas are particularly useful when operations are limited in scope and geographic area or when operations are to conducted on the boundaries between theaters. Also called JOA. See also joint special operations area. (JP 1-02)

military operations other than war. Operations that encompass the use of military capabilities across the range of military operations short of war. These military actions can be applied to complement any combination of the other instruments of national power and occur before, during and after war. Also called MOOTW. (JP 1-02) *{An umbrella term encompassing a variety of military operations conducted by the Department of Defense that normally complement the other instruments of*

national power. These military operations are as diverse as providing support and assistance (when consistent with US law) in a nonthreatening environment, and conducting combat not associated with war.} {Italicized definition in brackets applies only to the USAF and is offered for clarity} (AFDD 1)

operational control. Transferable command authority that may be exercised by commanders at any echelon at or below the level of combatant command. Operational control is inherent in combatant command. Operational control may be delegated and is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives and giving authoritative direction necessary to accomplish the missions assigned to the command. Operational control should be exercised through the commanders of subordinate joint force commanders and Service and / or functional component commanders. Operational control normally provides full authority to organize commands and forces and to employ those forces as the commander in operational control considers necessary to accomplish assigned missions. Operational control does not, in and of itself, include authoritative direction for logistics or matters of administration, discipline, internal organization or unit training. Also called OPCON. (JP 1-02)

operational effect. Link between tactical results and strategy; typically the cumulative outcome of mission, engagements and battles. Can also result from disruption of systems or areas of operational value. (AFDD 2-1)

OODA loop. A theory developed by Col John Boyd (USAF, ret) contending that one can depict all rational human behavior, individual and organizational, as a continual cycling through four distinct tasks: observation, orientation, decision and action. (AFDD 2-5)

parallel attack. Simultaneous attack of varied target sets to shock, disrupt or overwhelm an enemy, often resulting in decisive effects. Parallel attack is possible at one or multiple levels of war and achieves rapid effects that leave the enemy little time to respond. (AFDD 2-1)

peace enforcement. Application of military force, or the threat of its use, normally pursuant to international authorization, to compel compliance with resolutions or sanctions designed to maintain or restore peace and order. Also called PE. (JP 1-02)

peacekeeping. Military operations undertaken with the consent of all major parties to a dispute, designed to monitor and facilitate implementation of an agreement (ceasefire, truce, or other such agreement) and support diplomatic efforts to reach a long-term political settlement. Also called PK. See also peace enforcement; peace operations. (JP 1-02)

peace operations. A broad term that encompasses peacekeeping operations and peace enforcement operations conducted in support of diplomatic efforts to establish and maintain peace. Also called PO. See also peace enforcement. (JP 1-02)

psychological operations. Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning and ultimately the behavior of foreign governments, organizations, groups and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. Also called PSYOP. (JP 1-02)

reachback. The process of obtaining products, services and applications or forces, equipment or material from Air Force organizations that are not forward deployed. (AFDD-2)

reconnaissance. A mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy, or the secure data concerning the meteorological, hydrographic or geographic characteristics of a particular area. (JP 1-02)

rules of engagement. Directives issued by competent military authority that delineate the circumstances and limitations under which the United States forces will initiate and / or continue combat engagement with other forces encountered. Also called ROE. (JP 1-02)

shared data environment. Automation services that support the implementation and maintenance of data resources that are used by two or more combat support applications. Services provided include: identification of common data, physical data modeling, data base segmentation, development of data access and maintenance routines and data base reengineering to use the common data environment. (JP 1-02)

space control. Operations to assure the friendly use of the space environment while denying its use to the enemy. Achieved through offensive and defensive counterspace carried out to gain and maintain control of activities conducted in or through the space environment. (AFDD 1)

special operations. Operations conducted by specially organized, trained and equipped military and paramilitary forces to achieve military, political, economic or psychological objectives by unconventional military means in hostile, denied or politically sensitive areas. These operations are conducted during peacetime competition, conflict and war , independently or in coordination with operations of conventional, nonspecial operations forces. Political-military considerations frequently shape special operations, requiring clandestine, covert or low visibility techniques and oversight at the national level. Special operations differ from conventional operations in degree of physical and political task, operational techniques, mode of employment, independence from friendly support and dependence on detailed operational intelligence and indigenous assets. Also called SO. (JP 1-02)

strategic attack. Military action carried out against an enemy's center(s) of gravity or other vital target sets, including command elements, war production assets and key supporting infrastructure in order to effect a level of destruction and disintegration of the enemy's military capacity to the point where the enemy no longer retains the ability or will to wage war or carry out aggressive activity. (AFDD 1)

strategic effect. Disruption of the enemy's overall strategy, ability or will to wage war or carry out aggressive activity.

supported commander. The commander having primary responsibility for all aspects of a task assigned by the Joint Strategic Capabilities Plan or other joint operation planning, this term refers to the commander who prepares operation plans or operation orders in response to requirements of the Chairman of the Joint Chiefs of Staff. (JP 1-02)

supporting commander. A commander who provides augmentation forces or other support to a supported commander or who develops a supporting plan. Includes the

designated combatant commands and Defense agencies as appropriate. See also supported commander. (JP 1-02)

surveillance. The systematic observation of aerospace, surface or subsurface areas, places, persons or things by visual, aural, electronic, photographic or other means (JP 1-02)

synchronization. 1. The arrangement of military actions in time, space and purpose to produce maximum relative combat power at the decisive place and time. 2. In the intelligence context, application of intelligence sources and methods in concert with the operational plan. (JP 1-02)

tactical control. Command authority over assigned or attached forces or commands, or military capability or forces made available for tasking, that is limited to the detailed and, usually, local direction and control of movements or maneuvers necessary to accomplish missions or tasks assigned. Tactical control is inherent in operational control. Tactical control may be delegated to, and exercised at any level at or below the level of combatant command. Also called TACON. (JP 1-02)

target acquisition. The detection, identification and location of a target in sufficient detail to permit the effective employment of weapons. (JP 1-02)

target analysis. An examination of potential targets to determine military importance, priority of attack and weapons required to obtain a desired level of damage or casualties. (JP 1-02)

targeting. 1. The process of selecting targets and matching the appropriate response to them, taking account of operational requirements and capabilities. 2. The analysis of enemy situations relative tot he commander's mission, objectives and capabilities at the commander's disposal, to identify and nominate specific vulnerabilities that, if exploited, will accomplish the commander's purpose through delaying, disrupting, disabling or destroying enemy forces or resources critical to the enemy. (JP 1-02)

target system. 1. All the targets situated in a particular geographic area and functionally related. 2. A group of targets which are so related that their destruction will produce some particular effect desired by the attacker. (JP 1-02)

telecommunication. Any transmission, emission or reception of signs, signals, writings, images, sounds or information of any nature by wire, radio, visual or other electromagnetic systems. (JP 1-02)

unified action. A broad generic term that describes the wide scope of actions (including the synchronization of activities with governmental and nongovernmental agencies) taking place within unified commands, subordinated unified commands or joint task forces under the overall direction of commanders of those commands. (JP 1-02)

unified command plan. The document, approved by the President, which sets forth basic guidance to all unified combatant commanders; establishes their missions, responsibilities, and force structure; delineates the general geographical area of responsibility for geographic combatant commanders; and specifies functional responsibilities for functional combatant commanders. Also called UCP. (JP 1-02)

unity of command. A principle of War whose purpose is to ensure unity of effort under one responsible commander for every objective. All forces operate under a single commander with the requisite authority to direct all forces employed in pursuit of a common purpose. (JP 1)

unity of effort. A principle of Military Operations Other Than War that requires coordination and cooperation among all forces toward a commonly recognized objective, although they are not necessarily part of the same command structure. It is an essential complement to unity of command. (JP 1)

vulnerability. 1. The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. 2. The characteristics of a system which cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment. 3. In information operation, a weakness in information system security design, procedures, implementation or internal controls that could be exploited to gain unauthorized access to information or an information system. (JP 1-02)

vulnerability analysis. In information operations, a systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. (JP 1-02)

Bibliography

14th Air Force Mission Statement. n.p. On-line. Internet, 15 March 2002. Available from http://www.vandenberg.af.mil/associate_units/14af/index.html.

21st Space Wing Mission Statement. n.p. On-line. Internet, 15 March 2002. Available from http://131.15.144.52/21sw/.

67th Information Operations Wing Mission Statement. n.p. On-line. Internet, 15 March 2002. Available from https://aiaweb.aia.af.mil/homepages/67iow/67iw-hompage.html.

Air Force Doctrine Document (AFDD) 1. *Air Force Basic Doctrine*, September 1997.

Air Force Doctrine Document (AFDD) 2. *Organization and Employment of Aerospace Power*, 17 February 2000.

Air Force Doctrine Document (AFDD) 2-1. *Air Warfare*, 22 January 2000.

Air Force Doctrine Document (AFDD) 2-5. *Information Operations*, 22 January 2002.

Air Force Space Command Mission Statement. n.p. On-line. Internet, 15 March 2002. Available from http://www.spacecom.af.mil/hqafspc/goals/AFSPC2001PerformancePlan.htm.

Concept of Operations for Time Critical Targeting and Time Critical Strikes during Millenium Challenge 2002. Version 4.4. (MC CONOPS) AC2ISRC/C2N, Langley Air Force Base, VA. 14 September 2001

Diffie, Whitfield and Susan Landau. *Privacy on the Line: The Politics of Wiretapping and Encryption.* Cambridge, Massachusetts: The MIT Press. 1999.

Hoffer, Jeffrey A., Joey F. George and Joseph S. Valacich. *Modern Systems Analysis and Design.* Second Edition. Reading, Massachusetts: Addison Wesley Longman, Inc., 1999.

Joint Doctrine Capstone and Keystone Primer. 8 May 2001.

Joint Publication (JP) 0-2. *Unified Action Armed Forces. (UNAAF)*. 10 July 2001.

Joint Publication (JP) 1-02. *Department of Defense Dictionary of Military and Associated Terms.* 12 April 2001.

Joint Publication (JP) 2-0. *Doctrine for Intelligence Support to Joint Operations.* 9 March 2000.

Joint Publication (JP) 3-13. *Joint Doctrine for Information Operations.* 9 October 1998.

Laudon, Kenneth C. and Jane P. Laudon. *Essentials of Management Information Systems: Transforming Business and Management.* Third Edition. Upper Saddle River, N.J.: Prentice Hall, Inc., 1999.

McCrabb, Maris, Dr. *Concept of Operations for Effects-based Operations.* (EBO CONOPS). Version 2.0. Air Force Research Laboratory, 11 July 2000.

Myers, Richard C., General, USAF. 5 January 2000 Transcript from Department of Defense News Briefing, USCINCSPACE. n.p. On-line. Internet, 15 March 2002.

Available from http://www.defenselink.mil/news/Jan2000/t01052000_t104myer.html.
Pillsbury, Michael, ed. *Chinese Views of Future Warfare.* Revised Edition. Washington D.C.: National Defense University Press. September 1998.
Robbins, Stephen P. *Organization Theory: Structure, Design and Application.* Third Edition. Englewood Cliffs, N.J.: Prentice Hall, Inc., 1990.
Sharp, Walter Gary, Sr. *Cyberspace and the Use of Force.* United States: Aegis Research Corporation, 1999.
Sprague, Ralph H., Jr. and Barbara C. McNurlin. *Information Systems Management in Practice.* Third Edition. Englewood Cliffs, N.J.: Prentice Hall, Inc., 1993.
Standage, Tom. *The Victorian Internet: the remarkable story of the telegraph and the nineteenth century's on-line pioneers*. Walker Publishing Company, Inc. New York. 1998.
Stein, George J. "Information Warfare." *Aerospace Power Chronicles.* n.p. On-line. Internet, 8 November 2001. Available from http://www.airpower.au.af.mil/airchronicles/apj/stein.html.
Thomas, Timothy L. "Behind the Great Firewall of China: A Look at RMA/IW Theory from 1996-1998." Fort Leavenworth, KS: Foreign Military Studies Office. n.p. On-line. Internet, 8 November 2001. Available from http://call.army.mil/fmso/fmsopubs/issues/chinarma.htm.
Thomas, Timothy L. "Human Network Attacks." *Military Review*, September-October 1999. 1-14. Fort Leavenworth, KS: Foreign Military Studies Office. On-line. Internet, 8 November, 2001. Available from http://call.army.mil/fmso/fmsopubs/issues/humannet/humannet.htm.
Tzu, Sun. *The Art of War*. Translated by Samuel B. Griffith. New York, N.Y.: Oxford University Press, 1971.
USAF Concept of Operations for Aerospace Operations Center. (USAF AOC CONOPS). AC2ISRC/A31. Langley Air Force Base, VA. 9 March 2001.
USAF Information Warfare Mission Area Plan. (USAF IW MAP). Headquarters Air Combat Command. Langley Air Force Base, VA. March 2001.
Waltz, Edward. *Information Warfare: Principles and Operations*. Norwood, MA: Artech House, Inc., 1998.
Warden, John A., Colonel. “The Enemy as a System.” National Planning Systems and Joint Campaign Planning, Volume 6. pp 100-111. Air Command and Staff College: Maxwell Air Force Base, AL. January 2002.
Widnall, Sheila E., Secretary of the Air Force and General Ronald R. Fogleman. *Cornerstones of Information Warfare*. 1-13. On-line. Internet, 6 November 2001. Available from http://www.af.mil/lib/corner.html.